Deutscher Bundestag **Drucksache 19/517**

19. Wahlperiode 19.01.2018

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Dr. Petra Sitte, Simone Barrientos, Birke Bull-Bischoff, Anke Domscheit-Berg, Brigitte Freihold, Nicole Gohlke, Ulla Jelpke, Jan Korte, Cornelia Möhring, Norbert Müller (Potsdam), Zaklin Nastic, Sören Pellmann, Martina Renner, Kersten Steinke, Katrin Werner und der Fraktion DIE LINKE.

Nutzung von Verschlüsselung (TSL/SSL bzw. HTTPS) auf Internetseiten von Bundesbehörden

Bei Transport Layer Security (TLS; SSL ist die Bezeichnung eines Vorgängerprotokolls) handelt es sich um ein gängiges Verschlüsselungsprotokoll für Datenübertragung im Internet. Verwendet wird es unter anderem im Rahmen von HTTPS, einer verschlüsselten Version des Hypertext Transfer Protocol (HTTP), das insbesondere der Übertragung von Webseiten dient.

Die Verwendung von HTTPS zur Auslieferung von Webseiten hat zwei zentrale Vorteile: Sie gewährleistet Vertraulichkeit, da die übertragenen Daten (also der Inhalt der Seite und Eingaben wie etwa Zugangsdaten) verschlüsselt und damit der Einsicht durch Dritte entzogen sind; und sie gewährleistet Integrität, da sie Gewissheit über die Identität des Webseitenanbieters gibt und so Phishing- oder Man-in-the-Middle-Angriffen vorbeugen kann. Während in der Vergangenheit HTTPS vor allem im Rahmen bestimmter besonders sensibler Dienste wie etwa Zahlungstransaktionen verwendet wurde, hat es sich in den letzten Jahren immer mehr als allgemeiner Sicherheitsstandard etabliert und inzwischen erfolgt weltweit mehr als die Hälfte des Webverkehrs über HTTPS (www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web).

Seit 2014 existiert ein Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden, dessen Anwendung nach einer entsprechenden Verwaltungsvorschrift (GMBl 2015 S. 173) verbindlich ist und das in seiner Begründung insbesondere auf die Wichtigkeit der damit gewährleisteten sicheren Datenübertragung bei E-Government-Anwendungen verweist.

In ihrer Digitalen Agenda 2014 bis 2017 hat sich die Bundesregierung unter anderem das Ziel gesetzt, „die Kommunikation über digitale Netze zu schützen und dafür den Zugang zu sicheren und einfach zu nutzenden Verschlüsselungsverfahren zu fördern“ und Deutschland zum „Verschlüsselungs-Standort Nr. 1“ werden zu lassen. Dazu solle „die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden“.

Nach Recherchen der Open Knowledge Foundation Deutschland (zugänglich unter https://https.jetzt/) unterstützen von 513 untersuchten Domains deutscher Bundesbehörden mit Stand vom Januar 2018 lediglich 135, also etwa 26 Prozent, den Einsatz von HTTPS.

Wir fragen die Bundesregierung:

1. Teilt die Bundesregierung die Auffassung, dass der flächendeckende Einsatz von HTTPS im World Wide Web ein erstrebenswertes Ziel ist, um ein Höchstmaß an Sicherheit zu gewährleisten?
2. Welche Anstrengungen hat die Bundesregierung bisher unternommen, um im Sinne ihrer Digitalen Agenda die Verwendung von HTTPS bzw. des SSL/TLS-Protokolls insgesamt zu fördern?
3. Wie ist es nach Auffassung der Bundesregierung zu bewerten, dass allem Anschein nach nur ein geringer Anteil von Domains deutscher Bundesbehörden den Einsatz von HTTPS unterstützt?
4. Plant die Bundesregierung Maßnahmen, um diesen Anteil zu erhöhen, und wenn ja welche?
5. Wie viele Domains werden insgesamt von Bundesbehörden betrieben (aufgeschlüsselt nach Behörde und in Summe)?
   a) Auf wie vielen dieser Domains wird jeweils der Einsatz von HTTPS unterstützt?
   b) Auf wie vielen dieser Domains wird jeweils der Einsatz von HTTPS technisch erzwungen?
   c) Auf wie vielen dieser Domains ist jeweils das Protokoll HTTP Strict Transport Security (HSTS) implementiert?
6. Wie viele Verwaltungsdienstleistungen von Bundesbehörden werden über Weboberflächen erbracht (aufgeschlüsselt nach Behörde und in Summe)?
   a) Für wie viele davon wird jeweils der Einsatz von HTTPS unterstützt?
   b) Für wie viele davon wird jeweils der Einsatz von HTTPS technisch erzwungen?
   c) Für wie viele davon ist jeweils das HSTS-Protokoll implementiert?
7. Wie ist die von verschiedenen Bundesministerien vertretene Auffassung begründet, dass ein Zugang zu vollständigen Listen registrierter Domains nachteilige Auswirkungen auf Belange der inneren oder äußeren Sicherheit haben könne (vgl. https://fragdenstaat.de/anfrage/registrierte-domains-des-gesundheitsministeriums/#nachricht-45513), und welche konkreten Bedrohungsszenarien und Sicherheitskonzepte sind damit verbunden?

Berlin, den 19. Januar 2018

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333